

Draadloos internet, maar dan veilig

Zowat iedereen met breedbandinternet installeert meteen een draadloze WiFi-router. Comfort gegarandeerd: je kan van overal in het huis of de tuin surfen en struikelt niet over lelijke kabels. Maar standaard is zo'n draadloos netwerkje niet erg veilig. Wat moet je weten over beveiliging van draadloze netwerken, en hoe doe je het goed? FREDERICK GORDTS

Bestel je breedbandinternet via de kabel of ADSL, dan krijg je daar doorgaans een draadloze router bij. Handig, want zo kan je niet alleen je computers in je werkkamer verbinden met een kabel, maar ook draadloos met een laptop (of desktop) surfen in elke andere kamer van het huis, of zelfs in de tuin. WiFi stopt echter niet aan de buitenmuren van je huis of je tuin, zodat buren of toevallige passanten makkelijk je breedbandverbinding kunnen gebruiken om te surfen. En dat is een groot risico, want wat als je buurman mp3-bestanden ter beschikking stelt of dubieuze plaatjes downloadt via jouw breedbandverbinding? Wettelijk ben jij dan in de meeste gevallen aansprakelijk! Je draadloos netwerk beveiligen is eenvoudig, maar je doet het best meteen.

Risico's

De meeste draadloze routers worden standaard zonder beveiliging geleverd. Dat heeft een voordeel, want je kan meteen surfen en moet niet in de weer met wachtwoorden en sleutels. Maar het is natuurlijk onveilig. Niet alleen kunnen anderen meesurfen op je internetverbinding; hackers of crackers kunnen ook nagaan naar wie je mailt (en zelfs de inhoud zien) en waarheen je surft. En als je zonder wachtwoord mappen deelt in Windows, kunnen ze zelfs snuisteren op je pc!

Standaarden

WiFi-versleuteling is zo complex omdat er meerdere beveiligingsstandaarden bestaan. We zetten ze even op een rijtje:



- **WEP** of **Wired Equivalent Privacy** is de allereerste versleutelingsstandaard, maar wordt nog heel veel gebruikt. Het is een erg zwakke technologie, omdat de gebruikte sleutel "statisch" is en dus nooit wijzigt. Met bepaalde software kan je na een paar minuten de sleutel al "kraken" en alsnog meeluisteren of -surfen. WEP activeer je door in de router een sleutel (wachtwoord) in te stellen, en dat wachtwoord ook op elke pc in te geven in de instellingen van de draadloze netwerkkaart, zodat beide sleutels overeenstemmen.
- **WPA** of **WiFi Protected Access** maakt gebruik van een TKIP of Temporal Key Integrity Protocol, waarbij de sleutels op gezette tijdstippen automatisch worden gewijzigd.
- **WPA2** is de meest recente versleutelingsstandaard en is eigenlijk de enige definitieve standaard. Het gebruikt geen TKIP maar AES (Advanced Encryption Standard), dat gegarandeerd veilig zou zijn. Alle nieuwe netwerkkaarten en routers die sinds maart 2006 op de markt zijn, ondersteunen WPA2.

Zowel WPA als WPA2 werken met een sleutel, of liever: een *passphrase*. Dat is een langer wachtwoord, dat idealiter uit meerdere woorden (inclusief spaties en leestekens) en hoofd- en kleine letters bestaat. Dit wordt ook wel de PSK of *pre-shared key* modus genaamd. Serverauthenticatie (Radius) bestaat ook, maar daarvoor is een specifieke server vereist, zodat het enkel relevant is in grotere bedrijven.

Surf je al veilig?

Wil je nagaan of je al "veilig" draadloos surft, dan kan dat eenvoudig in Windows. Klik met de rechtermuisknop op het icoontje van het netwerk in het systeemvak van Windows XP (naast de klok). Als er een slotje naast je netwerk staat, dan is het beveiligd. Staat er ook WPA vermeld, dan

GOEIE BUREN?



Op een onbeveiligd draadloos netwerk kunnen de buren gewoon meesurfen.

gebruik je WPA- of WPA2-encryptie. Is dat niet het geval, dan gaat het om WEP.

Mogelijkheden van router en netwerkkaarten controleren

Wil je je netwerk versleutelen, of van WEP naar WPA(2) gaan, dan moet je eerst weten of je router en WiFi-netwerkkaarten WPA of WPA2 ondersteunen. In Windows XP ga je daarvoor naar **Start**, **Configuratiescherm**, **Netwerkverbindingen** en klik je met de rechtermuisknop op **Draadloze netwerkverbinding**. Kies **Eigenschappen** en ga naar het tabblad **Draadloze netwerken**. Klik onder **Voorkeursnetwerken** op **Toevoegen** en ga na of er WPA of WPA2 (AES) staat onder **Netwerkverificatie**. Druk daarna op **Annuleren**. Zie je geen WPA of WPA2 staan, ga dan naar de website van de fabrikant van je netwerkkaart of computer om na te gaan of er geen nieuwe stuurprogramma's zijn.
Vervolgens ga je naar de administratiepagina van je router. Die kan je met een browser meestal benaderen op het adres http://192.168.0.1, http://192.168.1.1 of http://10.0.0.1. Je moet inloggen met een wachtwoord, dat je vindt in het handboek van je router. Ga nu op zoek naar WLAN of WiFi security of encryption. Op de juiste pagina zie je meteen welke standaarden je router ondersteunt. Enkel WEP? Geen nood; een firmware-upgrade kan vaak WPA(2) toevoegen. Ga daarvoor naar de website van de fabrikant van de router.
Let wel op: een WiFi-netwerk versleutelen betekent vaak dat je moet experimenteren met instellingen. Hou een gewone netwerkkabel klaar voor als je draadloos niet meer op de router kan, om foute instellingen ongedaan te maken!

WPA of WPA2 instellen

Klaar? Dan kan je je router omzetten naar WPA(2). Stel in elk geval een moeilijk te raden passphrase in en probeer eerst de beste versleuteling uit (WPA2 met AES). Pas dit toe op de router en stel dit daarna in op je pc's. Draait alles goed, dan hou je het zo. Lukt het niet, probeer dan eens WPA met TKIP. Lukt ook dat niet, schakel dan over naar WEP, want dat is nog altijd beter dan geen versleuteling. ♦

802.11?

Koop je een WiFi-router of -kaart, dan wordt er gegoocheld met afkortingen. Eén ervan is 802.11. 802.11b, de "oudste" standaard uit 1999, haalt een snelheid van 11 Mbit/s. Daarna kwamen 802.11g (54 Mbit/s) en 802.11a (dezelfde snelheid maar amper gebruikt). Nu is er ook 802.11n (tot 540 Mbit/s), of toch niet? Hoewel je al heel wat routers kan kopen die 802.11n-compatibel zijn, klopt dat eigenlijk niet, want de 802.11n-standaard is nog niet definitief. De modellen die je nu koopt, zijn daarom "draft-n" of "pre-n" compatibel. Dat betekent zoveel als: compatibel met de n-standaard van het eigen merk, maar je krijgt geen garanties dat ze ook compatibel zijn met de nieuwe standaard, eens die er is. Ons advies: koop nog geen 802.11n-toestellen, maar hou het voorlopig bij de veel goedkopere 802.11g-standaard!